UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,682	10/25/2001	John Patrick McGregor JR.	10006270-1	3181

7590 11/07/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/001,682	MCGREGOR, JOHN PATRICK	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/25/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed August 8, 2005, have been fully considered but they are not persuasive.

2. Claims 1-19 are pending and have been examined.

Response to Amendment

3. The objection to the disclosure is withdrawn.

4. Regarding the independent claims, in response to applicant's arguments, the recitation "a method of reducing computation during each Data Encryption Standard encryption and decryption round" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

5. Adams et al. (US Patent Number 5,825,886, hereinafter "Adams") teaches the limitations' language, and is explicit regarding the use of the modifications to improve the Data Encryption Standard (columns 5-8). Adams further teaches using different operations to modify the round key computation that add security without degrading performance. Adams teaches enhancements to the round function of DES (columns 3-5) as does the claimed invention. Menezes et al. teach on page 259 that the speed of DES implementations can be improved through very large lookup tables.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-3, 8-12, and 17-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Adams.

Regarding claim 1, Adams et al. teach

- a) generating at least one large SP-box lookup table (column 5, lines 23-34);
- b) computing an index for each SP-box lookup table (column 5, lines 51-67);
- c) adding operations to the DES round key computation function to obtain a modified round key computation function (column 5, lines 34-40, column 6, lines 33-67); and
- d) computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function (column 5, lines 51-67).

Regarding claim 2, Adams et al. teach

- a) generating at least one large SP-box lookup table (column 5, lines 23-34);
- b) adding operations to the DES round key computation function to obtain a modified round key computation function (column 5, lines 34-40, column 6, lines 33-67);

- c) computing a modified SP-box index by performing XOR operations between at least one block of contiguous bits of the 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function of step b) (column 5, lines 51-67); and
- d) executing each subsequent round of DES computation by repeating steps a) and c) (column 5, lines 23-34).

Regarding claim 3, Adams et al. teach wherein steps a) through d) are carried out in a digital processor (column 8, lines 8-15).

Regarding claim 8, Adams et al. teach mathematically transforming the DES round function in each said round; mathematically transforming the DES round key computation function in each said round; and modifying the inputs to said SP-boxes in accordance with the results of steps a) and b) (column 6, lines 33-67, column 7, lines 1-30).

Regarding claim 9, Adams et al. teach wherein steps a) and b) are carried out so that computation in the DES Expansion Permutation is shifted from the DES round function to the DES round key computation function (column 6, lines 51-62).

Regarding claim 10, Adams et al. teach

- a) means for generating at least one large SP-box lookup table (column 5, lines 23-34);
- b) means for computing an index for each SP-box lookup table (column 5, lines 51-67);

- c) means for adding operations to the DES round key computation function to obtain a modified round key computation function (column 5, lines 34-40, column 6, lines 33-67); and
- d) means for computing the index for each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function (column 5, lines 51-67).

Regarding claim 11, Adams et al. teach

- a) means for generating at least one large SP-box lookup table (column 5, lines 23-34);
- b) means for adding operations to the DES round key computation function to obtain a modified round key computation function (column 5, lines 51-67);
- c) means for computing a modified SP-box index by performing XOR operations between at least one selected block of said 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function (column 5, lines 51-67).

Regarding claim 12, Adams et al. teach wherein said means for computing comprises a digital processor (column 8, lines 8-15).

Regarding claim 17, Adams et al. teach means for mathematically transforming the DES round function in each said round; means for mathematically transforming the DES round key computation function in each said round; and means for modifying the inputs to said SP-boxes in accordance with the transformations of said round function

and of said round key computation function (column 6, lines 33-67, column 7, lines 1-30).

Regarding claim 18, Adams et al. teach wherein means for modifying comprises means for shifting computation in the DES Expansion Permutation from the DES round function to the DES round key computation function (column 6, lines 51-62).

Regarding claim 19, Adams et al. teach a data processing system for carrying out Data Encryption Standard (DES) encryption and decryption rounds with reduced computation, the system comprising:

- a) computer processing means for processing data (column 4, lines 55-59);
- b) storage means providing four large SP-box lookup tables (figure 2);
- c) means for computing indices for the respective SP-box lookup tables (column 5, lines 51-67);
- d) means for adding operations to the DES round key computation function to obtain a modified round key computation function (column 5, lines 34-40, column 6, lines 33-67); and
- e) means for computing the index of each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function (column 5, lines 51-67).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams as applied to claims 3 and 12 respectively above, and further in view of Candelore (US Patent Number: 5,861,662).

Regarding claims 4 and 13, Adams teaches the limitations as set forth under claims 3 and 12 respectively above. Adams does not disclose expressly wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor. However, Candelore teaches wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor (column 6, lines 12-26). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use digital processor taken from the group consisting of a general-purpose processor, an embedded processor, and a cryptographic processor. One of ordinary skill in the art would have been motivated to use such processors to provide a wide range of possible implementations.

10. Claims 5-7 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams as applied to claims 2 and 11 respectively above, and

further in view of Menezes et al. (NPL Handbook of Applied Cryptography, pages 252-256).

Regarding claim 5, Adams teaches the limitations as set forth under claim 2 above. Adams does not disclose expressly wherein step c) comprises the step of selecting two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation. However, Menezes et al. teach wherein step c) comprises the step of selecting two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation (page 252). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation. One of ordinary skill in the art would have been motivated to do so since it is part of the algorithm for the Data Encryption Standard.

Regarding claim 6, the combination of Adams and Menezes et al. teaches the limitations as set forth under claim 5 above. Furthermore, Menezes et al. teach wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round (page 252).

Regarding claim 7, Adams teaches the limitations as set forth under claim 2 above. Adams does not disclose expressly wherein step c) is carried out by permuting the entries within each SP-box lookup table. However, Menezes et al. teach wherein step c) is carried out by permuting the entries within each SP-box lookup table (page 253). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to permute the entries within each SP-box lookup table as is done in DES. One of ordinary skill in the art would have been motivated to do so since it is part of the algorithm for the Data Encryption Standard.

Regarding claim 14, Adams teaches the limitations as set forth under claim 11 above. Adams does not disclose expressly wherein said means for computing comprises means for selecting two blocks of said 32-bit input to the DES Expansion Permutation. However, Menezes et al. teach wherein said means for computing comprises means for selecting two blocks of said 32-bit input to the DES Expansion Permutation (page 252). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation. One of ordinary skill in the art would have been motivated to do so since it is part of the algorithm for the Data Encryption Standard.

Regarding claim 15, the combination of Adams and Menezes et al. teaches the limitations as set forth under claim 14 above. Furthermore, Menezes et al. teach wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round (page 252).

Regarding claim 16, Adams teaches the limitations as set forth under claim 11 above. Adams does not disclose expressly wherein said means for generating comprises means for permuting the entries within each said SP-box lookup table. However, Menezes et al. teach wherein said means for generating comprises means for

permuting the entries within each said SP-box lookup table (page 253). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to permute the entries within each SP-box lookup table as is done in DES. One of ordinary skill in the art would have been motivated to do so since it is part of the algorithm for the Data Encryption Standard.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

13. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

14. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100